IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: **DELLMO ET AL.**	
Serial No. **10/806,668**	Examiner: J. Pan
Confirmation No. **1171**	Art Unit: 2135
Filing Date: **March 23, 2004**	
For: **MODULAR CRYPTOGRAPHIC DEVICE PROVIDING STATUS DETERMINING FEATURES AND RELATED METHODS**	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the final Official Action of September 18, 2009, and in connection with the Notice of Appeal filed concurrently herewith, please consider the remarks set out below.

I. The Claims Are Patentable

The Examiner rejected independent Claims 1, 11, 21, 25, and 29 over Dhir et al. in view of Cheng in further view of Hamlin et al. Applicants submit that even a selective combination of the prior art fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Dhir et al. is directed to a programmable integrated circuit, namely a field programmable gate array (FPGA), that can

be used to handle different wireless local area network (WLAN) communication specifications. The Examiner correctly acknowledges that Dhir et al. fails to teach a cryptographic module and a communications module that are removably coupled to one another, and a cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner then turned to Cheng for one of these critical deficiencies.

Cheng is directed to an add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks. The add-on card includes an access control circuit, volatile and non-volatile memory, a wireless transmission module, and a network connection module. The network connection module has both an antenna for communicating with a wireless network, and a standard network cable port for connecting to a wired network. (See, e.g., paragraphs 0009-0010 of Cheng).

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner turned to Hamlin for this critical deficiency. Hamlin is directed to a device including encryption circuitry enabled by comparing an operating spectral signature to an initial spectral signature.

Applicants submit that the Examiner mischaracterized Hamlin, as it fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic

processor based upon tampering with the first housing. The Examiner contended that Col. 4, lines 5-8, of Hamlin, which are reproduced below for reference, somehow disclose the claimed cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing:

> "Attempts to tamper with the device 2 which alter the measured spectral characteristic of the clock signal 20 will disable the encryption circuitry 4 and prevent chosen plaintext attacks."

Indeed, Hamlin merely discloses disabling encryption circuitry based upon an alteration of a measured spectral characteristic of a clock signal or other internal signal. The measured spectral "characteristic may be, for example, a DC component of a power signal 20, or the convolution of such signals." (See Hamlin, Col. 4, lines 11-14). Nowhere does Hamlin disclose or suggest the cryptographic module includes a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Applicants further submit that a person having ordinary skill in the art would not recognize the recitations of "tampering or probing with the device" in the context of changing the spectral characteristic of a clock signal or a power signal, as teaching a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing. Accordingly, Hamlin fails to disclose a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing, as recited in the independent claims.

Additionally, the Examiner, in the Response to Arguments section of the Final Official Action dated September 18, 2009, recognized that Hamlin fails to explicitly disclose tampering with the first housing. The Examiner contended that Cheng discloses a housing, and thus a combination of Hamlin and Cheng discloses teaching a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing. Applicants submit that while Cheng may disclose a housing, even a selective combination of Hamlin and Cheng fails to disclose a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing.

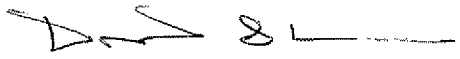
Instead, a combination of Hamlin and Cheng would result in the tamper circuit being included in the housing of Cheng, and any disabling encryption circuitry based upon an alteration of a measured spectral characteristic of a clock signal or other internal signal, and not tampering with the housing. In other words, tampering of a housing in a combination of Hamlin and Cheng would not result in disabling the cryptographic processor unless the tampering altered a measured spectral characteristic of a clock signal or other internal signal. A person having ordinary skill in the art would not combine Hamlin and Cheng to arrive at the claimed cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. Indeed, the Examiner is merely attempting to combine disjoint pieces of the prior art using Applicants' Specification as a roadmap for combination.

Applicants further submit that the Examiner's combination of Dhir et al., Cheng, and Hamlin is improper, as a

person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Hamlin to arrive at the claimed invention. More particularly, as an initial matter, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit board (330), as illustrated in Fig. 8 of Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board.

Accordingly, it is submitted that independent Claims 1, 11, 21, 25, and 29 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorney for Applicants